TASK FORCE WEB

Single Sign On (SSO) Update

9 July 2002

LCDR Armistead, TFW IA Team Lead
Christopher Hall, IT-21 IA Coordinator

Outline

- Why is SSO important?
- Fleet SSO Requirements
- Laboratory Testing
- Enterprise Standards
- SAML Discussion and Summary
- Fleet SSO Pilot
- SSO Demo
- Developer Impacts

Why is SSO Important?

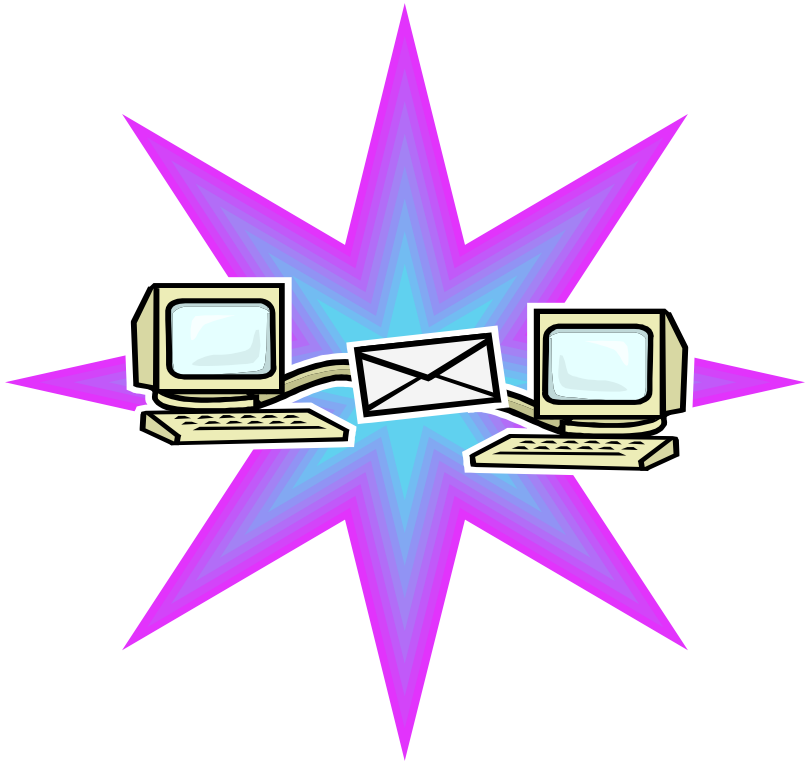
- Security Administration Management
- Identification and Authorization
- Access Control
- Data Integrity/ Confidentiality/ Encryption

Fleet SSO Requirements

- Fleet requirements comprise four major areas
  - Security
  - Deployability
  - Admin Functionality & Supportability
  - End-to-End SSO Interoperability

Laboratory Testing

- Laboratory testing was conducted by SSC-SD on NIPRNET and SIPRNET apps hosted within the NMCI enclave for the purpose of understanding interoperability issues associated with SSO
- Results were concluded on 28 June 2002



Enterprise Standards

- Security Assertion Markup Language (SAML) is an emerging XML based enterprise standard that provides SSO interoperability.
- SAML defines three types of security assertions:
  - Authentication, Attributes and Authorization
- SAML is still relatively immature, however:
  - Enables the exchange of authentication and authorization information between sites that have separate user directories and authorization policies in a coherent/uniform manner.
  - Supports the distribution of additional information (e.g., group/role information) about the user.

Enterprise Standards

- SAML reached “Committee Specification” maturity level on 16 April 2002.
- SAML has the potential to provide interoperability between shipboard and shore identity domains.
  - Shipboard user identities will be identical in shipboard and shore directories, but will actually be different objects. Joe.user34 must be able to retain the same identity in both security/identity domains to view both shipboard and shore applications simultaneously.
- SAML Authentication Assertions allow the shipboard SSO to authenticate Joe.user34 and assert to the shore SSO that he is Joe.user34 ashore as well.

SAML Interop 2002

- SAML vendors will participate in a SAML Interoperability Demonstration at the Burton Group Catalyst Conference 15-17 July 2002.
- Numerous SAML compliant product releases are expected to follow the Interop Conference.
- TFW is following SAML as an emerging standard for potential use at the enterprise implementation.
  - A final decision to incorporate SAML will be made after the industry standard is formalized.

SSO Summary

- A commercial standards based E2EMD Navy enterprise SSO solution does not exist today.
- Significant issues remain for an E2E SSO solution.
  - Retention of user Authentication and Authorization across multiple AD forests/identity domains.
  - Proven capability based on OASIS SAML 1.0 interoperability standard.

Fleet SSO Pilot

- TFW is not ready to endorse SSO products or select an enterprise SSO solution at this time.
- The Fleet has volunteered to test an SSO solution within a single security domain (not an end-to-end solution).
  - A pre-SAML implementation based on XML has been selected for this initial test.
  - The objective is it will provide a good understanding of the Navy's enterprise environment upon which to base an end-to-end SSO implementation.

The Bottom Line

- TFW will continue to monitor SAML developments.
- Developers must be of SSO and SAML capabilities and the associated implications in development of applications and services.

What does this mean to you as a Developer?

- You should be aware that future apps that are web-enabled will need an SSO plug-in.
- A pre-SAML SSO product is being explored for the 2BG rollout.
- Include SSO/SAML in your coding strategy!

Questions and Demo of SSO Product